C. AMENDMENTS TO THE CLAIMS

In order to better assist the Examiner with the prosecution of the case, the current pending claims have been included in their entirety for which allowance is requested. This listing of claims will replace all prior versions, and listings, of claims in the application.:

1. (Currently Amended) A method for predicting fraudulent identification usage, comprising:

responsive to detecting authentication of an identity of a user via a communication line into a same identification used to singly represent said user within a network environment comprising a trusted telephone network and a packet switching network communicatively connected via a secure channel to said trusted telephone network, detecting a context for use of said identification by a context inference service executing within said packet switching network, wherein said context inference service is enabled to detect use of said same identification in association with a plurality of purchases within said network environment comprising at least one of an in-store purchase, an internet purchase, and a telephone purchase and in association with a plurality of non-purchase uses of said network environment comprising at least one of a phone call and an internet service access;

detecting, at said fraud protection service, [[a]] said context for [[a]] use of said [[an]] identification via [[a]] said communication line from said context inference service[[at a fraud protection service]];

analyzing, at said fraud protection service, said context for use of said identification in view of a plurality of entries for use of said identification each previously received by said fraud protection service from said context inference service, wherein each of said plurality of entries comprises a previously detected context for use of said identification for one from among said plurality of purchases and said plurality of non-purchase uses within said network environment; and

specifying, by said fraud protection service, a level of suspicion of fraudulent use of said identification according to said analysis of said context.

2. (Original) The method for predicting fraudulent identification usage according to claim 1, wherein said identification comprises at least one from among a caller identity, an account number, a service number, and a password.

3. (Canceled).

4. (Canceled).

5. (Original) The method for predicting fraudulent identification usage according to claim 1, wherein said context comprises at least one from among an identity of a caller, an identity of a callee, a device utilized by said caller, a device utilized by said callee, an inferred location of said caller, a scheduled location of said caller, an inferred location of said callee, a scheduled location of said callee, an on behalf of party, a billing plan, an order placed, a service requested for access, and a subject.

6. (Original) The method for predicting fraudulent identification usage according to claim 5, wherein said inferred location of said caller and said callee further comprises a global positioning system location, a street address, a geographical area, a business location, and a home location.

7. (Currently Amended) The method for predicting fraudulent identification usage according to claim [[1]]5, wherein said billing plan further comprises at least one from among a service provider, an account provider and at least one shipping address.

8. (Original) The method for predicting fraudulent identification usage according to claim 1, wherein said use of said identification comprises at least one from among accessing a service from a service provider identified by said identification and placing an order with payment to an account provider identified by said identification.

9. (Canceled).

10. (Canceled).

11. (Canceled).

12. (Canceled).

13. (Canceled).

14. (Original) The method for predicting fraudulent identification usage according to claim 1, wherein analyzing said context for use of said identification further comprises:

analyzing said context in view of a fraud value associated with said context.

15. (Original) The method for predicting fraudulent identification usage according to claim 1, wherein analyzing said context for use of said identification further comprises:

accessing a schedule of events associated with said identification; and

comparing a location for origination of use of said identification in said context with said schedule of events.

16. (Original) The method for predicting fraudulent identification usage according to claim 1, further comprising:

responding to said level of suspicion according to a preference designated by a provider included in said context.

17. (Original) The method for predicting fraudulent identification usage according to claim 1, further comprising:

responding to said level of suspicion according to a preference designated by an owner of said identification.

18. (Original) The method for predicting fraudulent identification usage according to claim 1, further comprising:

controlling access to additional authentication of said identification.

19. (Currently Amended) A system for predicting fraudulent identification usage, comprising:

a fraud protection service server communicatively connected to a network environment comprising a trusted telephone network and a and a packet switching network communicatively connected via a secure channel to said trusted telephone network;

a context inference service server executing within said packet switching network, with means, responsive to detecting authentication of an identity of a user via a communication line into a same identification used to singly represent said user within said network environment, for detecting a context for use of said identification, wherein said context inference service is enabled to detect use of said same identification in association with a plurality of purchases within said network environment comprising at least one of an in-store purchase, an internet purchase, and a telephone purchase and in association with a plurality of non-purchase uses of said network environment comprising at least one of a phone call and an internet service access;

said fraud protection service server further comprising means for detecting [[a]] said context for [[a]] use of [[an]] said identification via [[a]] said communication line from said context inference service server [[at said fraud protection service server]];

said fraud protection service server further comprising means for analyzing said context for use of said identification in view of a plurality of entries for use of said identification each previously received by said fraud protection service from said context inference service, wherein each of said plurality of entries comprises a previously detected context for use of said identification for one from among said plurality of purchases and said plurality of non-purchase uses within said network environment;; and

said fraud protection service server further comprising means for specifying a level of suspicion of fraudulent use of said identification according to said analysis of said context.

20. (Original) The system for predicting fraudulent identification usage according to claim 19, wherein said identification comprises at least one from among a caller identity, an account number, a service number, and a password.

21. (Canceled).

22. (Canceled).

23. (Original) The system for predicting fraudulent identification usage according to claim 19, wherein said context comprises at least one from among an identity of a caller, an identity of a callee, a device utilized by said caller, a device utilized by said callee, an inferred location of said caller, a scheduled location of said caller, an inferred location of said callee, a scheduled location of said callee, an on behalf of party, a billing plan, an order placed, a service requested for access, and a subject.

24. (Currently Amended) The system for predicting fraudulent identification usage according to claim [[5]]23, wherein said inferred location of said caller and said callee further comprises a global positioning system location, a street address, a geographical area, a business location, and a home location.

25. (Currently Amended) The system for predicting fraudulent identification usage according to claim [[19]]23, wherein said billing plan further comprises at least one from among a service provider, an account provider and at least one shipping address.

26. (Original) The system for predicting fraudulent identification usage according to claim 19, wherein said use of said identification comprises at least one from among accessing a service from a service provider identified by said identification and placing an order with payment to an account provider identified by said identification.

27-31 (Canceled).

32. (Original) The system for predicting fraudulent identification usage according to claim 19, wherein said means for analyzing said context for use of said identification further comprises:

means for analyzing said context in view of a fraud value associated with said context.

33. (Original) The system for predicting fraudulent identification usage according to claim 19, wherein said means for analyzing said context for use of said identification further comprises:

means for accessing a schedule of events associated with said identification; and

means for comparing a location for origination of use of said identification in said context with said schedule of events.

34. (Original) The system for predicting fraudulent identification usage according to claim 19, further comprising:

means for responding to said level of suspicion according to a preference designated by a provider included in said context.

35. (Original) The system for predicting fraudulent identification usage according to claim 19, further comprising:

means for responding to said level of suspicion according to a preference designated by an owner of said identification.

36. (Original) The system for predicting fraudulent identification usage according to claim 19, further comprising:

means for controlling access to additional authentication of said identification.

37. (Currently Amended) A computer program product for predicting fraudulent identification usage, comprising:

a recording medium;

means, recorded on said recording medium, for detecting a context for use of an identification by a context inference service executing within a packet switching network, responsive to detecting authentication of an identity of a user via a communication line into said same identification used to singly represent said user within a network environment comprising a trusted telephone network and said packet switching network communicatively connected via a secure channel to said trusted telephone network, wherein said context inference service is enabled to detect use of said same identification in association with a plurality of purchases within said network environment comprising at least one of an in-store purchase, an internet purchase, and a telephone purchase and in association with a plurality of non-purchase uses of said network environment comprising at least one of a phone call and an internet service access;

means, recorded on said recording medium, for detecting [[a]] said context for [[a]] use of said [[an]] identification via [[a]] said communication line from said context inference service

means, recorded on said recording medium, for analyzing said context for use of said identification in view of a plurality of entries for use of said identification each previously received by said fraud protection service from said context inference service, wherein each of said plurality of entries comprises a previously detected context for use of said identification for one from among said plurality of purchases and said plurality of non-purchase uses within said network environment; and

means, recorded on said recording medium, for specifying a level of suspicion of fraudulent use of said identification according to said analysis of said context.

38. (Original) The computer program product for predicting fraudulent identification usage according to claim 37, further comprising:

means, recorded on said recording medium, for analyzing said context in view of a fraud value associated with said context.

39. (Original) The computer program product for predicting fraudulent identification usage according to claim 37, further comprising:

means, recorded on said recording medium, for accessing a schedule of events associated with said identification; and

means, recorded on said recording medium, for comparing a location for origination of use of said identification in said context with said schedule of events.

40. (Original) The computer program product for predicting fraudulent identification usage according to claim 37, further comprising:

means, recorded on said recording medium, for responding to said level of suspicion according to a preference designated by a provider included in said context.

41. (Original) The computer program product for predicting fraudulent identification usage according to claim 37, further comprising:

means, recorded on said recording medium, for responding to said level of suspicion according to a preference designated by an owner of said identification.

42. (Original) The computer program product for predicting fraudulent identification usage according to claim 37, further comprising:

means, recorded on said recording medium, for controlling access to additional authentication of said identification.

43-61 (Canceled).